II. CLAIM AMENDMENTS

Please amend the claims as indicated in the following listing:

1. Canceled.

2. Canceled.

3. Canceled.

4. Canceled.

5. Canceled.

6. Canceled.

7. Canceled.

8. Canceled.

9. Canceled.

10. Canceled.

11. Canceled.

12. Canceled.

13. Canceled.

14. Canceled.

15. Canceled.

16. Canceled.

17. (Currently Amended) A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing the firewall and a switch to service each of the plurality of computer networks by performing the steps of:

determining ~~the~~ a destination of the packet from a packet header;

accessing a plurality of rules;

determining the appropriate rules to use to analyze the packet;

analyzing the packet using the rules;

determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, permitting the packet to pass to the destination;

responsive to a determination that the rules deny the packet, denying the packet;

wherein a trust level is a security level associated with a particular set of rules in the firewall; and

~~wherein a residence time is the time required for the firewall to analyze and either permit or deny the packet; and~~

wherein the trust level reduces the time required for the firewall to analyze and either permit or deny the packet ~~residence time of the packet in the firewall~~.

18. (original) The method of claim 17 further comprising: responsive to a determination that the rules do not permit or deny the packet, denying the packet.

19. (Previously Presented) The method of claim 17 wherein a table defines the relationship between the plurality of trust levels, the rules, and the computer networks.

20. (Currently amended) A method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing the firewall and a plurality of sub-switches to service each of the plurality of computer networks by performing the steps of:

determining ~~the~~ a sub-switch location of a packet;

determining a source and a destination of the packet from a packet header;

~~determining a destination of the packet;~~

determining if the packet is attempting to go to a destination with a higher trust level than a trust level of the source; and

responsive to a determination that the packet is not attempting to go to a higher trust level, permitting the packet to pass to the destination;

wherein a trust level is a security level associated with a particular set of rules in the firewall; and

~~wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet; and~~

wherein the trust level reduces the time required for the firewall to analyze and either permit or deny a packet ~~residence time of the packet in the firewall~~.

21. (original) The method of claim 20, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the method further comprises:

determining the appropriate rules to use to analyze the packet using the table;

analyzing the packet using the rules;

determining if the packet is permitted under the rules;

responsive to a determination that the rules permit the packet, permitting the packet; and

responsive to a determination that the rules deny the packet, denying the packet.

22. (original) The method of claim 21 wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, denying the packet.

23. (original) The method of claim 20 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks.

24. Canceled.

25. Canceled.

26. Canceled.

27. Canceled.

28. Canceled.

29. Canceled.

30. Canceled.

31. Canceled.

32. Canceled.